

Catalogue de services et Formations

EXUNOV est une société de conseil, de formation et d'ingénierie en Système d'Information et en Sécurité des Systèmes d'Information.



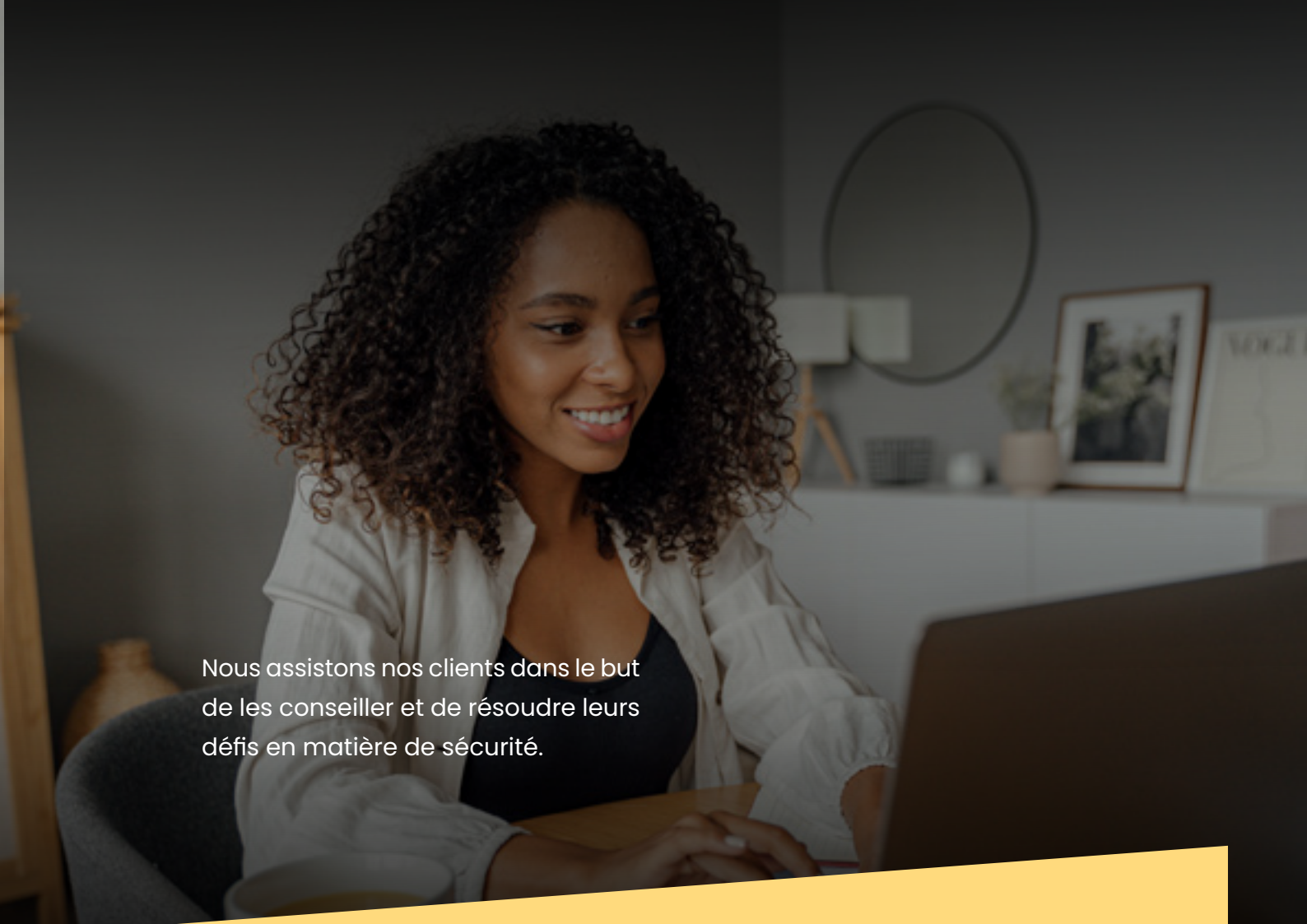
Présentation de l'entreprise

Depuis sa création, l'offre globale solutions (produits et services) d'EXUNOV est restée centrée sur les solutions de sécurité informatique des entreprises et n'a cessé de s'enrichir en intégrant les innovations technologiques afin de répondre aux besoins de ses clients et d'être toujours en avance dans un monde en perpétuelle mutation.

Grâce à ses experts en sécurité, EXUNOV aide ses clients à garantir la sécurité de leurs données, apporte un appui aux petites et moyennes entreprises par le biais d'une assistance informatique et d'une gestion efficace des services informatiques. Nous assistons nos clients dans le but de les conseiller et de résoudre leurs défis en matière de sécurité.

Grâce à nos quatre lignes de services intégrés (Conseil, Cybersécurité, Conformité et la Formation) et à notre connaissance approfondie du secteur, EXUNOV aide ses clients à tirer parti des nouvelles opportunités, à évaluer et gérer les risques pour assurer une croissance responsable puis à former les équipes informatiques et audit interne.

Nos équipes multidisciplinaires très performantes et notre approche conseils nous permettent de répondre aux préoccupations des entreprises tout en respectant les exigences réglementaires.



Nous assistons nos clients dans le but de les conseiller et de résoudre leurs défis en matière de sécurité.

Notre vision est de devenir le plus important fournisseur de services informatiques et de sécurité des Systèmes d'Information en Afrique de l'Ouest

Mission de l'entreprise



Sécuriser

EXUNOV vous accompagne sur l'ensemble des phases de votre projet de la rédaction de la Politique de Sécurité du Système d'Information (PSSI)



Industrialiser

Mettre en oeuvre l'automatisation nécessaire pour les phases de détection et de remédiation.



Simplifier

Faciliter la gestion des changement. Simplifier l'administration et l'exploitation de vos infrastructures de sécurité.



Innover

Notre pôle R&D assure une veille technologique sur les dernières solutions, et développe ses propres solutions.

Nos équipes multidisciplinaires très performantes et notre approche conseils nous permettent de répondre aux préoccupations des entreprises tout en respectant les exigences réglementaires.

Nos services



CONSEIL

Nous vous accompagnons pour analyser, réaliser ou piloter vos projets informatiques ou, d'une façon plus globale, pour optimiser vos processus internes grâce au numérique.

- ▶ Missions d'expertise métier
- ▶ Assistance à maîtrise d'ouvrage
- ▶ Conseils opérationnels

[En savoir plus →](#)

CYBER-SÉCURITÉ

Nous vous conseillons et vous aidons à déployer un ensemble de moyens techniques, organisationnels et humains pour garantir la sécurité de votre système d'information.

- ▶ Gouvernance
- ▶ Audits de sécurité
- ▶ Pentests
- ▶ Sensibilisation des collaborateurs

[En savoir plus →](#)



CONFORMITÉ ISO/IEC 27001

Pour la sécurité internationale nous vous accompagnons dans le cadre du contrôles de gestion des risques techniques requis pour un système de gestion de la sécurité de l'information (ISMS).

- ▶ CONFORMITE ISO/IEC 27001
- ▶ Investigation numérique

[En savoir plus →](#)

Notre Démarche



**QUALIFICATION
DU BESOIN**



**SÉLECTION
DU CONSULTANT**



**PROPOSITION
DU PROFIL ET ENTRETIEN**



**VALIDATION DE
LA MISSION ET DU
CONSULTANT**



**DÉMARRAGE
DE LA MISSION**



**SUIVI
DE LA MISSION**

| Nos offres de formation

Isaca

- ▶ CISM
- ▶ CISA
- ▶ CRISC

PEBC

- ▶ iso 27001 lead auditor
- ▶ iso 27001 lead implementor

Autres

- ▶ CEH v11
- ▶ CISSP
- ▶ ITIL v4



Préparation à la certification CISM

Certified Information Security Manager

Objectifs de cette formation

- ▶ Maîtriser les quatre grands domaines de la gestion de la sécurité conformes à la certification CISM.
- ▶ Maîtriser le vocabulaire et les principes de l'examen de certification.
- ▶ Maîtriser l'ensemble des méthodes et des normes internationales en matière de gestion de la sécurité de l'information.

Programme

MODULE 1 : LA GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION

Ce module est consacré au premier domaine de la certification CISM, l'ensemble des méthodes et pratiques de la gestion de la sécurité de l'information selon l'ISACA.

- ▶ Concilier les stratégies de sécurité de l'information avec la stratégie de l'organisation
- ▶ Développer une politique de sécurité de l'information performante
- ▶ Répartir les rôles et les responsabilités au sein de la gouvernance
- ▶ Audit, information et communication autour de la gouvernance de la sécurité

MODULE 2 : GÉRER LES RISQUES IT ET LA CONFORMITÉ

Ce module revient sur les questions du deuxième domaine de la certification CISM, à savoir la gestion des risques pesant sur le système de sécurité, et la conformité des processus.

- ▶ Mettre en place une approche systématique et analytique, et un processus continu de gestion des risques
- ▶ Identifier, analyser et évaluer les risques
- ▶ Définir des stratégies de traitement des risques
- ▶ Mettre en place une communication effective autour de la gestion des risques

MODULE 3 : DÉVELOPPER ET GÉRER UN PLAN DE SÉCURITÉ IT

Conforme au troisième domaine de l'examen CISM, ce module aborde les questions de mise en place des plans de sécurité de l'information.

- ▶ Comprendre l'architecture de la sécurité de l'information
Méthodologie et pratiques pour mettre en place des mesures de sécurité
Gérer les contrats et les prérequis de la sécurité de l'information
- ▶ Utiliser les métriques et évaluer la performance de la sécurité

Module 4 : Gérer les incidents de la sécurité de l'information

Le dernier domaine du CISM s'intéresse à la gestion des éventuels incidents touchant la sécurité de l'information d'une organisation, via un ensemble de méthodes et pratiques.

- ▶ Fonctionnement du plan de gestion des incidents de sécurité
- ▶ Pratiques et techniques de la gestion des incidents de sécurité
- ▶ Méthode de classification
- ▶ Les processus de notification et d'escalade
- ▶ Détecter et analyser les incidents



SECURITY

Préparation à la certification CISA

Certified Information System Auditor

Objectifs de cette formation

- ▶ Approfondir vos connaissances et améliorer vos compétences en audit des systèmes d'information
- ▶ Analyser et maîtriser les différents domaines sur lesquels porte l'examen du CISA
- ▶ Assimiler le vocabulaire et les idées directrices de l'examen CISA
- ▶ S'entraîner au déroulement de l'examen et acquérir les stratégies de réponse au questionnaire

Programme

DOMAINE 1 : PROCESSUS D'AUDIT DES SI (21%)

- ▶ Les standards de l'audit.
- ▶ L'analyse des risques ainsi que le contrôle interne
- ▶ Pratiquer l'auto-évaluation
- ▶ Réaliser un audit du Système d'Information

DOMAINE 2 : GOUVERNANCE ET GESTION DES TI (16%)

- ▶ La gouvernance
- ▶ La stratégie de la gouvernance
- ▶ Le Risk management.
- ▶ L'audit de la gouvernance.
- ▶ Plans de continuité et de secours (SMCA)
- ▶ Réaliser un audit du SMCA

DOMAINE 3 : ACQUISITION, CONCEPTION ET IMPLANTATION DES SYSTÈMES D'INFORMATION (18%)

- ▶ Cycle de vie des systèmes et de l'infrastructure.
- ▶ Pratique et audit d'un projet
- ▶ Le développement
- ▶ L'audit de la maintenance applicative et des systèmes.
- ▶ Les différents contrôles applicatifs.

DOMAINE 4 : EXPLOITATION, ENTRETIEN ET GESTION DES SYSTÈMES D'INFORMATION (20%)

- ▶ L'audit de l'exploitation des SI.
- ▶ L'audit des aspects matériels du SI.
- ▶ L'audit des architectures SI et réseaux.

DOMAINE 5 : PROTECTION DES AVOIRS INFORMATIQUES (25%)

- ▶ La gestion de la sécurité : politique et gouvernance.
- ▶ L'audit et la sécurité logique et physique.
- ▶ L'audit de la sécurité des réseaux. L'audit des dispositifs nomades.



Préparation à la certification CRISC

Certified in Risk and Information Systems Control

Objectifs de cette formation

- ▶ Maîtriser les quatre grands domaines de la gestion de la sécurité conformes à la certification CISM.
- ▶ Maîtriser le vocabulaire et les principes de l'examen de certification.
- ▶ Maîtriser l'ensemble des méthodes et des normes internationales en matière de gestion de la sécurité de l'information.

Programme

MODULE 1 : VUE D'ENSEMBLE DU CRISC

- ▶ Présentation générale du CRISC
- ▶ Déroulement de l'examen

MODULE 2 : IDENTIFIER, ANALYSER ET ÉVALUER LE RISQUE

- ▶ Les normes en vigueur sur la gestion des risques
- ▶ Les référentiels de la gestion des risques
- ▶ Comprendre la gestion des risques en entreprise
- ▶ Connaître les différents niveaux de risque en entreprise
- ▶ Identifier les risques
- ▶ Analyser et évaluer les risques
- ▶ Analyses quantitatives et qualitatives

MODULE 3 : RÉPONDRE AU RISQUE

- ▶ Méthodologie de traitement des risques
- ▶ Mitigation des risques, contrôle du système d'information
- ▶ Réduire les risques
- ▶ Transférer le risque
- ▶ Accepter les risques résiduels
- ▶ Mettre en place des plans de traitement des risques

MODULE 4 : SURVEILLER LE RISQUE

- ▶ Le cycle de vie du traitement des risques
- ▶ Surveiller les risques traités
- ▶ Surveiller les risques résiduels
- ▶ Evaluer la performance de la gestion des risques, rapporter les risques
- ▶ Les Key Risk Indicators (indicateurs clés de risques)

MODULE 5 : CONTRÔLER LE SYSTÈME D'INFORMATION

- ▶ Définir les contrôles
- ▶ Mettre en place des contrôles du système d'information
- ▶ Mesurer les processus et les services de contrôle du système d'information

MODULE 6 : LE CYCLE DE VIE DES CONTRÔLES DU SYSTÈME D'INFORMATION

- ▶ Planifier des stratégies de gestion du cycle de vie des contrôles du SI
- ▶ Définir le périmètre, les enjeux et les avantages des plans de gestion du cycle de vie des contrôles
- ▶ Assurer une surveillance permanente des contrôles
- ▶ Maintenir les contrôles du système d'information
- ▶ Assurer l'amélioration continue de la gestion des risques et des contrôles



Préparation à la certification ISO 27005 Risk Manager

Risk Manager

Objectifs de cette formation

- ▶ Connaître la relation entre la gestion des risques et sécurité SI
- ▶ Maîtriser la norme ISO 27005 pour pouvoir analyser des risques du système d'information
- ▶ Se préparer et passer l'examen de certification «Risk Manager ISO 27005»

Programme

PRÉSENTATION DE LA FAMILLE DES NORMES ISO 2700X

PRÉSENTATION DE LA NORME ISO 27005

- ▶ Évaluation, traitement, acceptation du risque
- ▶ Communication
- ▶ Gestion et revue du risque

POSITIONNEMENT DE LA STRATÉGIE DE GESTION DE RISQUE

Selon ISO 27005 vis à vis du processus de management de la sécurité du système d'information SMSI (ISO 27001)

DÉFINITION D'UNE STRATÉGIE DE GESTION DES RISQUES

- ▶ Définition de l'approche d'appréciation du risque
- ▶ Identification, analyse et évaluation des risques
- ▶ Identification et évaluation des choix de traitement des risques
- ▶ Sélection des mesures de sécurité
- ▶ Approbation des risques résiduels

STRATÉGIE D'APPRÉCIATION DU RISQUE

Identification des actifs et propriétaires, des menaces, vulnérabilités, impacts

STRATÉGIE DE TRAITEMENT DU RISQUE

- ▶ Évaluation du risque
- ▶ Choix de traitement des risques
- ▶ Choix des mesures de sécurité

PROCESSUS DE SUIVI ET REVUE DES RISQUES

- ▶ Indicateurs de suivi
- ▶ Comité de pilotage opérationnel et comité stratégique de la sécurité
- ▶ Approbation des risques résiduels

ETUDE DE CAS

PASSAGE DE LA CERTIFICATION



Préparation à la certification CEH v11

Certified Ethical Hacking

Objectifs de cette formation

- ▶ Développer des compétences spécifiques en système et réseau informatique
- ▶ Connaître et maîtriser les outils d'hacking
- ▶ Maîtriser les méthodologies de piratage et d'intrusion éthique
- ▶ Comprendre les lois et l'éthique forte à respecter pour toute personne certifiée CEH
- ▶ Connaître et réaliser une démarche d'audit sécurité

Programme

PRÉSENTATION DU PIRATAGE ÉTHIQUE (ETHICAL HACKING)

- ▶ Profil et motivation d'un pirate
- ▶ Différence avec un pirate éthique

MÉTHODES, TECHNIQUES ET OUTILS DE PIRATAGE

- ▶ Biométrie
- ▶ Analyse de réseaux, systèmes

- ▶ Piratage de système et réseau
- ▶ Attaque de système et réseau
- ▶ Pénétration de système et réseau
- ▶ Piratage d'identifiant et de session
- ▶ Utilisation de SQL pour pirater un système
- ▶ Attaque de site internet et d'applications
- ▶ Détection de vulnérabilités et faiblesses de systèmes tiers
- ▶ Hacking et Cloud computing
- ▶ Cryptographie et chiffrement
- ▶ Utilisation de virus et type de virus
- ▶ Ingénierie sociale

AUDIT

- ▶ Méthode et processus d'audit

LOI ET ÉTHIQUE

- ▶ Présentation des lois
- ▶ Information sur l'éthique appliquée au piratage informatique certifié CEH



Préparation à la certification ISO 27001 Lead Auditor

Lead Auditor

Objectifs de cette formation

- ▶ Connaître le fonctionnement d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO /CEI 27001
- ▶ Connaître le fonctionnement d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO /CEI 27001
- ▶ Être en mesure de planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011

Programme

INTRODUCTION AU SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

- ▶ Objectifs et structure de la formation
- ▶ Cadres normatifs et réglementaires : organisation et principes de base de l'ISO, système de management intégré, normes en sécurité de l'information, avantages de l'ISO27001
- ▶ Processus de certification : schéma de certification, autorité d'accréditation, organisme de certification
- ▶ Principes fondamentaux du Système de Management de la Sécurité de l'Information
- ▶ Définition et mise en oeuvre d'un SMSI

PRINCIPES, PRÉPARATION ET DÉCLENCHEMENT DE L'AUDIT

- ▶ Principes et concepts fondamentaux d'audit : normes d'audit, types d'audits, acteurs, objectifs et critères de l'audit, audit combinée
- ▶ Approche d'audit fondée sur les preuves
- ▶ Approche d'audit fondée sur le risque
- ▶ Déclenchement de l'audit : revue de la demande, nomination d'un responsable, validation des objectifs, du périmètre et des critères d'audit
- ▶ Étape 1 de l'audit : objectif, visite des lieux, entretiens, revue de la documentation, rapport d'audit
- ▶ Préparation de l'étape 2 de l'audit (audit sur site) : préparation du plan d'audit, assignation des auditeurs, recours aux experts techniques, préparation des documents de travail, utilisation d'une liste de contrôle, mise en place d'une norme de documentation
- ▶ Étape 2 de l'audit (première partie) : conduire la réunion d'ouverture, collecter des informations, conduire les tests d'audits avec les procédures appropriées, rédiger des constats d'audits et des rapports de non-conformité

ACTIVITÉS D'AUDIT SUR SITE

- ▶ Étape 2 de l'audit (deuxième partie) : rédiger des constats d'audit et de non-conformité, exécuter la revue qualité des constats d'audit
- ▶ Communication pendant l'audit : comportement pendant les visites sur site, communication durant l'audit, réunions de l'équipe d'audit, rôles des guides et observateurs, gestion des conflits, aspects culturels de l'audit, communication avec la direction
- ▶ Rédaction des plans de tests d'audit
- ▶ Rédaction des constats d'audit et des rapports de non-conformité

CLÔTURE DE L'AUDIT

- ▶ Documentation de l'audit et revue de qualité de l'audit : documents de travail, enregistrements d'audits, revue de qualité, documentation de la revue de qualité
- ▶ Clôture de l'audit : préparation des conclusions, discussion des conclusions avec l'audité, réunion de clôture, rapport d'audit, audit de suivi, décision de certification, contenu d'un certificat

- ▶ Évaluation des plans d'actions par l'auditeur : dépôt des plans d'actions par l'audit, contenu des plans d'action, évaluation des plans d'action
- Suite de l'audit initial : activité de surveillance, audit de surveillance, audit de renouvellement, utilisation des marques déposées ISO
- ▶ Management d'un programme d'audit interne : particularités de l'audit interne, indépendance et impartialité, le rôle de la fonction de l'audit interne, ressources et outils de l'audit interne, surveillance du programme
- ▶ Compétence et évaluation des auditeurs : qualification, compétences des responsables d'équipes d'audit, schéma de certification, certification, maintien de la certification

PASSAGE DE L'EXAMEN "PECB ISO 27001 LEAD AUDITOR"

- ▶ Révision des concepts en vue de la certification et examen blanc
Un voucher permettant le passage du test de certification est adressé à l'issue de la session
- ▶ Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
- ▶ Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
- ▶ Toutes les étapes sont détaillées [ici](#)
- ▶ Passage de l'examen de certification en français en 3 heures
- ▶ Un score minimum de 70% est exigé pour réussir l'examen
- ▶ Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- ▶ Les candidats sont autorisés à utiliser les supports de cours et les normes ISO/IEC 27001 et ISO/IEC 27002 qui leurs seront remises
- ▶ En cas d'échec ils bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative

L'examen couvre les domaines de compétences suivants :

- Domaine 1 : Principes et concepts fondamentaux du SMSI
- Domaine 2 : Le SMSI
- Domaine 3 : Principes et concepts fondamentaux de l'audit
- Domaine 4 : Préparation d'un audit ISO/CEI 27001
- Domaine 5 : Réalisation d'un audit ISO/CEI 27001
- Domaine 6 : Clôturer un audit ISO/CEI 27001
- Domaine 7 : Gérer un programme d'audit ISO/CEI 27001



Préparation à la certification ISO 27001 Lead Implementer

Lead Implementer

Objectifs de cette formation

- ▶ Comprendre la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires
- ▶ Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en oeuvre et gérer efficacement un SMSI
- ▶ Savoir interpréter les exigences de la norme ISO/CEI 27001 dans un contexte spécifique de l'organisation
- ▶ Savoir accompagner une organisation dans la planification, la mise en oeuvre, la gestion, la surveillance et la tenue à jour du SMSI

Programme

INTRODUCTION À LA NORME ISO/CEI 27001 ET INITIALISATION D'UN SMSI

- ▶ Objectifs et structure de la formation
- ▶ Cadres normatifs et réglementaires
- ▶ Système de Management de la Sécurité de l'Information
Principes et concepts fondamentaux du Système de Management de la Sécurité de l'Information
- ▶ Initialisation de la mise en oeuvre du SMSI
- ▶ Compréhension de l'organisation et clarification des objectifs de sécurité de l'information
- ▶ Analyse du système de management existant

PLANIFICATION DE LA MISE EN OEUVRE D'UN SMSI

- ▶ Leadership et approbation du projet du SMSI
- ▶ Périmètre du SMSI
- ▶ Politiques de sécurité de l'information
- ▶ Appréciation du risque
- ▶ Déclaration d'applicabilité et décision de la direction pour la mise en oeuvre du SMSI
- ▶ Définition de la structure organisationnelle de la sécurité de l'information

MISE EN OEUVRE D'UN SMSI

- ▶ Définition d'un processus de gestion de la documentation
- ▶ Conception des mesures de sécurité et rédaction des procédures et des politiques spécifiques
- ▶ Plan de communication
- ▶ Plan de formation et de sensibilisation
- ▶ Mise en oeuvre des mesures de sécurité
- ▶ Gestion des incidents
- ▶ Gestion des activités opérationnelles

SURVEILLANCE, MESURE, AMÉLIORATION CONTINUE ET PRÉPARATION DE L'AUDIT

- ▶ Surveillance, mesure, analyse et évaluation
- ▶ Audit interne
- ▶ Revue de direction
- ▶ Traitement des non-conformités
- ▶ Amélioration continue
- ▶ Préparation de l'audit de certification
- ▶ Compétence et évaluation des "Implementers"
- ▶ Clôture de la formation

PASSAGE DE L'EXAMEN "PECB ISO 27001 LEAD IMPLEMENTER"

- ▶ Révision des concepts en vue de la certification et examen blanc
- ▶ Un voucher permettant le passage du test de certification est adressé à l'issue de la session
- ▶ Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
- ▶ Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
- ▶ Toutes les étapes sont détaillées sur <https://pecb.com/help/wp-content/uploads/2018/07/Guide-de-pr%C3%A9paration-a-l%E2%80%99examen-en-ligne-de-PECB.pdf>
- ▶ Passage de l'examen de certification en français en 3 heures
- ▶ Un score minimum de 70% est exigé pour réussir l'examen
- ▶ Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- ▶ Les candidats sont autorisés à utiliser non seulement les supports de cours mais aussi les normes ISO/IEC 27001 et ISO/IEC 27002 qui leurs seront remises
- ▶ En cas d'échec les candidats bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative



Préparation à la certification CISSP

Certified Information Systems Security Professional

Objectifs de cette formation

- ▶ Connaître les différents domaines du CBK défini par l'(ISC)² ;
- ▶ Obtenir les connaissances fondamentales concernant la sécurité des systèmes d'information et la gestion des risques ;
- ▶ Être bien préparé pour le passage l'examen officiel CISSP

Programme

INTRODUCTION À LA SÉCURITÉ DU SI ET DU CBK DE L'(ISC)²

- ▶ La sécurisation des systèmes d'information.
- ▶ La certification CISSP®.
- ▶ L'étendue du CBK (Common Body of Knowledge).

INTRODUCTION À LA SÉCURITÉ DU SI ET DU CBK DE L'(ISC)²

- ▶ Les pratiques liées à la gestion de la sécurité.
- ▶ La gestion des risques et le programme de management.
- ▶ Les mesures préventives.
- ▶ L'amélioration des pratiques d'embauche.
- ▶ Les systèmes d'exploitation (OS).

CRYPTOGRAPHIE

- ▶ Les concepts de la cryptographie.
- ▶ Les types de cryptographie.
- ▶ La sécurité de développement d'applications.
- ▶ Les bases de données.

SÉCURISATION DES TÉLÉCOMMUNICATIONS ET DES RÉSEAUX

- ▶ Les notions de base.
- ▶ Les protocoles de sécurité.
- ▶ Les technologies WAN.
- ▶ La sécurisation d'un réseau Ethernet.
- ▶ La sécurité avec un pare-feu.

SÉCURISATION DES INFORMATIONS ET GESTIONS DES RISQUES

- ▶ Les mesures d'urgence.
- ▶ La sécurité physique.
- ▶ Les rôles et les responsabilités.
- ▶ Le module DSLC.
- ▶ Les procédures après sinistre.

CONSEILS ET ASTUCES POUR L'EXAMEN CISSP



Préparation à la certification ITILv4

ITILv4

Objectifs de cette formation

- ▶ Comprendre les concepts clés de la gestion des services
- ▶ Comprendre comment les principes directeurs d'ITIL peuvent aider une organisation à adopter et à adapter la gestion des services
- ▶ Comprendre les quatre dimensions de la gestion des services
- ▶ Comprendre le but et les composants du système de valeur des services ITIL
- ▶ Comprendre les activités de la chaîne de valeur des services, et leurs interconnexions

Programme

AVANT LA SESSION

Pour aborder la formation dans les meilleures conditions, retrouvez sur le Learning Hub ib : Un quiz de validation des pré-requis

CONCEPTS CLÉS DE LA GESTION DES SERVICES

- ▶ Gestion des services, valeur et service
- ▶ Organisations et co-crédation de valeur
- ▶ Les rôles de consommateur de services
- ▶ Configurer des ressources pour la création de valeur
- ▶ Offres de service
- ▶ Relations de service
- ▶ Valeur, résultats, coûts et risques
- ▶ Comprendre l'utilité et la garantie

SYSTÈME DE VALEUR DES SERVICES (SVS)

- ▶ Vue d'ensemble
- ▶ Opportunité, demande, valeur
- ▶ Principes directeurs
- ▶ Gouvernance 30
- ▶ Chaîne de valeur des services (SVC)
- ▶ Pratiques
- ▶ Amélioration continue

PRINCIPES DIRECTEURS ITIL

- ▶ Vue d'ensemble
- ▶ Privilégier la valeur
- ▶ Commencez là où vous êtes
- ▶ Avancer par itérations avec des retours
- ▶ Collaborer et promouvoir la visibilité
- ▶ Penser et travailler de façon holistique
- ▶ Opter pour la simplicité et rester pratique
- ▶ Optimiser et automatiser

QUATRE DIMENSIONS DE LA GESTION DES SERVICES

- ▶ Vue d'ensemble
- ▶ Dimension "organisations et personnes"
- ▶ Dimension "partenaires et fournisseurs"
- ▶ Dimension "flux de valeur et processus"
- ▶ Dimension "information et technologie"
- ▶ Facteurs externes

CHAÎNE DE VALEUR DES SERVICES ITIL (SVC)

- ▶ Vue d'ensemble Activité "Planifier"
- ▶ Activité "Améliorer"
- ▶ Activité "Impliquer"
- ▶ Activité "Conception et Transition"
- ▶ Activité "Obtenir/Construire"
- ▶ Activité "Fournir et Soutenir"
- ▶ Exemple de modèle de flux de valeur "Développement d'un nouveau service"
- ▶ Exemple de modèle de flux de valeur "Restauration d'un service en production"

PRATIQUES DE GESTION GÉNÉRALE

- ▶ Vue d'ensemble
- ▶ Pratique d'amélioration continue
- ▶ Pratique de gestion de la sécurité de l'information
- ▶ Pratique de gestion des relations
- ▶ Pratique de gestion des fournisseurs

PRATIQUES DE GESTION DES SERVICES

- ▶ Vue d'ensemble
- ▶ Pratique de gestion des niveaux de service
- ▶ Pratique de gestion des actifs informatiques
- ▶ Pratique de gestion de la configuration des services
- ▶ Pratique de surveillance et de gestion des évènements
- ▶ Pratique de centre de services
- ▶ Pratique de gestion des demandes de service
- ▶ Pratique de gestion des incidents
- ▶ Pratique de gestion des problèmes
- ▶ Pratique d'habilitation des changements
- ▶ Pratique de gestion des mises en production

PRATIQUES DE GESTION DES SERVICES

- ▶ Vue d'ensemble
- ▶ Pratique de gestion des déploiements

PRÉPARATION ET PASSAGE DE LA CERTIFICATION

- ▶ Révision des concepts en vue de la certification
- ▶ Jeux de questions/réponses
- ▶ Examen blanc
- ▶ Correction collective



Préparation à la Formation Cybercriminalité – Enjeux et défis

Cybercriminalité – Enjeux et défis

Objectifs de cette formation

- ▶ Comprendre les enjeux de la cybercriminalité
- ▶ Être capable d'identifier les biens essentiels à protéger
- ▶ Pouvoir identifier les sources de risques dans son organisation
- ▶ Comprendre comment détecter des actes de malveillance
- ▶ Savoir réagir face à un acte de malveillance

Programme

L'ÉVOLUTION DE LA CYBERCRIMINALITÉ

- ▶ Internet aujourd'hui, données et chiffres
- ▶ Les nouveaux marchés de la cybercriminalité
- ▶ Approche économique de la cybercriminalité
- ▶ Comprendre le darknet
- ▶ Les outils des cybercriminels (botnets, attaques etc...)
- ▶ Quelques typologies d'attaque

DROIT DES TIC ET ORGANISATION DE LA CYBERSÉCURITÉ

- ▶ Organisation de la cybersécurité en France
- ▶ Contexte juridique
- ▶ Droit des TIC
- ▶ La lutte contre la cybercriminalité, ANSSI et cybermalveillance
- ▶ Le rôle de la CNIL et la protection des données personnelles

PROTÉGER SON ORGANISATION

- ▶ Lexique et définitions (vulnérabilités, menaces, risques...)
- ▶ Les enjeux des Systèmes d'Information
- ▶ Identifier les biens essentiels et les biens supports
- ▶ Intégrer la sécurité au sein de son organisation
- ▶ Intégrer la sécurité au sein d'un projet
- ▶ Identification des difficultés liées à la prise en compte de la sécurité

IDENTIFIER ET PRÉVENIR LES SOURCES DE RISQUES

- ▶ Gouvernance et cybersécurité, définition des rôles et responsabilités
- ▶ Définir une stratégie de sécurité des systèmes d'information
- ▶ La Charte Informatique
- ▶ La gestion des contrats
- ▶ Mettre en place un système de gestion des risques
- ▶ Aperçu des ISO 27001 et 27005

PRÉVENIR LES RISQUES : LES BONNES PRATIQUES

- ▶ Les contrôles d'accès (physiques, logiques...)
- ▶ La gestion des comptes administrateurs
- ▶ La gestion des mots de passe
- ▶ Gérer les développements, les mises à jours et les déploiements
- ▶ Mettre en place une procédure d'escalade d'incidents
- ▶ Procédures ANSSI et CNIL de déclaration d'actes de malveillance



Préparation à la Formation Sensibilisation à la cybersécurité

Cybercriminalité - Enjeux et défis

Objectifs de cette formation

- ▶ Découvrir les bonnes pratiques pour limiter les risques juridiques et opérationnels
- ▶ Comprendre comment protéger les informations en adéquation avec les besoins métiers

Programme

INTRODUCTION

- ▶ Les préjugés à surmonter
- ▶ Les valeurs essentielles à protéger
- ▶ Les périmètres
- ▶ Les menaces

L'ORGANISATION ET LES RESPONSABILITÉS

- ▶ La direction générale
- ▶ Les directions métiers
- ▶ La DSI
- ▶ Les sous-traitants
- ▶ La voie fonctionnelle SSI et le RSSI
- ▶ La voie fonctionnelle protection de la vie privée et le DPO
- ▶ Les administrateurs techniques et fonctionnels
- ▶ Les utilisateurs

LES RÉFÉRENTIELS SSI ET VIE PRIVÉE

- ▶ Les politiques
- ▶ Les chartes
- ▶ Les guides et manuels
- ▶ Les procédures

VISION SYNTHÉTIQUE DES OBLIGATIONS LÉGALES

- ▶ Disciplinaire
- ▶ Contractuelle
- ▶ Civiles
- ▶ Pénales
- ▶ Le cas du contrôle par l'employeur : utilisation professionnelle et non-professionnelle

VISION SYNTHÉTIQUE DES OBLIGATIONS LÉGALES

- ▶ La divulgation d'information "spontanée"
- ▶ L'ingénierie sociale et l'incitation à dire ou faire
- ▶ Le lien avec l'intelligence économique
- ▶ Le lien avec l'espionnage industriel

LES RISQUES

- ▶ Vol, destruction
- ▶ Virus
- ▶ Les aspirateurs à données
- ▶ Le phishing /l'hameçonnage
- ▶ Les malwares
- ▶ Les spywares
- ▶ L'usurpation
- ▶ L'usurpation
- ▶ Les virus
- ▶ Le cas des réseaux sociaux

LES BONNES PRATIQUES D'ÉVALUATION DE LA SENSIBILITÉ DE L'INFORMATION

- ▶ La classification par les impacts, (juridiques, opérationnels, financiers, image, sociaux)
- ▶ L'échelle d'impact
- ▶ Les pièges

LES BONNES PRATIQUES POUR LES COMPORTEMENTS GÉNÉRAUX

- ▶ A l'intérieur des établissements
- ▶ A l'extérieur des établissements

LES BONNES PRATIQUES D'UTILISATION DES SUPPORTS D'INFORMATION SENSIBLE

- ▶ Papier
- ▶ Environnement partagé
- ▶ Environnement individuel sédentaire
- ▶ Environnement individuel mobile

LES BONNES PRATIQUES D'UTILISATION DES SUPPORTS D'INFORMATION SENSIBLE

- ▶ Installation et maintenance : postes fixes, équipements nomades, portables, ordiphones
- ▶ Identification et authentification
- ▶ Échanges et communications : intranet, internet, contrôle des certificats serveurs, les échanges de fichiers via la plate-forme "institutionnelle", le nomadisme, les télétravailleurs et le VPN de télé accès, email, la consultation en Web mail, signature, chiffrement, Cloud, réseaux sociaux et forums thématiques professionnels et privés, téléphonie
- ▶ Stockages et sauvegardes (clés usb, locales, serveurs, ...)
- ▶ Archivages
- ▶ Anonymisation
- ▶ Destruction ou recyclag

CONCLUSION

Les engagements de responsabilité



Formation Sécurité informatique : vocabulaire, concepts et technologies pour non-initiés

Comprendre la sécurité informatique

Objectifs de cette formation

- ▶ Comprendre les concepts, les technologies et les solutions de sécurité des réseaux informatiques pour travailler avec les spécialistes et piloter les prestataires
- ▶ Acquérir la vision globale de la sécurité
- ▶ Connaître les rôles des intervenants du secteur et leurs métiers
- ▶ Identifier les nouveaux enjeux associés à la sécurité informatique

Programme

PRINCIPES GÉNÉRAUX DE LA SÉCURITÉ INFORMATIQUE

- ▶ Domaines concernés : intégrité, disponibilité, confidentialité, authentification, imputation, traçabilité...
- ▶ Démarche générale à entreprendre / analyse de risques
- ▶ Notions à connaître : authentification simple et forte - Système de confirmation 3D, défense en profondeur, PRA/PCA...

COMPRENDRE LES DIFFÉRENTS TYPES DE VULNÉRABILITÉS ET D'ATTAQUES

- ▶ Malwares : cheval de Troie, Virus, Rootkit, Spyware...
- ▶ Attaques : terminal, réseaux, applications (Sniffing, DCI/DCI, DDoS...)
- ▶ Attaques de mots de passe, injection SQL, vol d'identité et de données
- ▶ Attaques non-malwares : attaques de phishing (hameçonnage)
- ▶ Évaluation des risques

CONNAÎTRE LE FONCTIONNEMENT DES ÉQUIPEMENTS DE PROTECTION DÉDIÉS

- ▶ Solution de gestion des mots de passe
- ▶ Cryptage : triple DES / AES
- ▶ Séparation des flux par la formation des réseaux virtuels (VLAN)
- ▶ Cryptage des données en ligne (VPN SSL et VPN IPSec)
- ▶ Authentification d'accès : authentification forte, Network Access Control (NAC) et Role Based Access Control (RBAC)
- ▶ Filtrage : firewalls protocolaires, de contenus, d'applications, d'identité...
- ▶ Filtrage des applications Web : WAF (Web Access Firewall)
- ▶ SIEM (Security Information and Event Management)
- ▶ IAM (Identity et Access Management)
- ▶ DLP (Data Lost Prevention) – Data Masking – Cryptage
- ▶ Empreintes logicielles et MAC (Mandatory Access Control)
- ▶ Autres domaines spécifiques

EXPLOITER LES PLATES-FORMES SPÉCIALISÉES DE SÉCURITÉ

- ▶ Plate-forme de Cloud de Sécurité (SecaaS : Security as a Service)
- ▶ Plate-forme de gestion et de sécurité des mobiles EMM (Enterprise Mobility Management)
- ▶ Plate-forme de sécurité NGFW (Next Generation of Firewall)

UTILISER LA COMBINAISON DES ÉQUIPEMENTS POUR SÉCURISER

- ▶ L'Internet (communication et transaction) : cryptologie PKI (Public Key Infrastructure)
- ▶ Les réseaux sans-fil Wifi : 802.11i (802.1X/EAP...) / WPA / WPA2 / WPA3
- ▶ Terminaux et applications mobiles et le télétravail (ODE, conteneurisation, App Stores, empreintes logicielles, App Wrapping...) / Banalisation du terminal et publication d'application (TS-WEB, VDI...)
- ▶ Le BYOD (utilisation des équipements personnels dans le cadre professionnel)
- ▶ La protection du Cloud et du Big Data (encryptions, vol de données, flux de données...)

MESURER LES IMPACTS DE LA MISE EN PLACE DE LA SÉCURITÉ

- ▶ La performance du système global du système informatique
- ▶ L'architecture du système d'information

S'APPUYER SUR LES RÉFÉRENTIELS POUR GÉRER LA SÉCURITÉ INFORMATIQUE

- ▶ ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information
- ▶ CSA (Cloud Alliance Security) / CSA Big Data / CSA Mobile
- ▶ CNIL/RGPD (Obligation Légale de sécurité)
- ▶ Critères communs
- ▶ CVE

GRANDES TENDANCES

- ▶ Limites des solutions actuelles de sécurité
- ▶ Cybersécurité : recours à l'intelligence artificielle et à la machine learning
- ▶ Security Self Healing System et Software Defined Security
- ▶ BlockChain



Formation État de l'art de la sécurité des Systèmes d'Information

Définition de la politique de sécurité et maîtrise des risques

Objectifs de cette formation

- ▶ Identifier les différents domaines de la sécurité et de la maîtrise des risques liés aux informations
- ▶ Connaître les principes et les normes de chaque domaine de la SSI
- ▶ Disposer d'informations sur les tendances actuelles au niveau des menaces et des solutions à notre disposition
- ▶ Pouvoir améliorer la communication entre la maîtrise d'ouvrage, la maîtrise d'oeuvre et la SSI
- ▶ Être en mesure d'effectuer des choix techniques

Programme

INTRODUCTION

ÉVOLUTIONS DES MENACES ET LES RISQUES

- ▶ Statistiques sur la sécurité
- ▶ Tendances dans l'évolution des menaces

MODÈLE D'APPROCHE ET MATURITÉ EFFECTIVE DE L'ORGANISME

- ▶ Identification des acteurs : organisation et responsabilités
Exigences SSI : obligations légales métiers, responsabilités civiles,
- ▶ responsabilités pénales, règlements, délégations

L'IDENTIFICATION DES BESOINS DICP CONSÉCUTIFS AUX ENJEUX

- ▶ Classification SSI : informations, données et documents, processus, ressources, les pièges
- ▶ Identification des menaces et des vulnérabilités : contextuelles métiers, contextuelles IT
- ▶ Cartographie des risques : gravité / vraisemblance, niveaux, traitement du risque, validation des risques résiduels

L'ÉTAT DE L'ART DES MÉTHODOLOGIES ET DES NORMES

- ▶ Bonnes pratiques SSI : les acteurs, les textes de référence, avantages et inconvénients ; les règles d'hygiène ANSSI, les fiches CNIL, le chapitre 7 RGS
- ▶ Approche enjeux : les acteurs, les textes de référence, avantages et inconvénients ; ISO 27002
- ▶ Approche SMSI : les acteurs, les textes de référence, avantages et inconvénients ; ISO 27001

MODÉLISATION DES NIVEAUX DE MATURITÉ DES TECHNOLOGIES SSI

- ▶ Les choix structurants et non structurants et positionnements dans la courbe de la pérennité
- ▶ La sécurité des accès : filtrage réseau, identification, authentification (faible, moyenne, forte), gestion des identités vs. SSO, habilitation, filtrage applicatif (WAF, CASB et protection du Cloud), détection/protection d'intrusion, journalisation, supervision
- ▶ La sécurité des échanges : algorithmes, protocoles, combinaisons symétriques et asymétriques TLS, certificats, IGCP, les recommandations ANSSI
- ▶ Infrastructures de clés publiques : autorités de certification et d'enregistrement, révocation
- ▶ Le cas du DLP : architecture

NOMADISME

- ▶ Sécurité des postes nomades : problèmes de sécurité liés au nomadisme
Protection d'un poste vs. solutions spécifiques
- ▶ Mise en quarantaine
- ▶ Accès distants
- ▶ VPN : concept et standards de VPN sécurisé, intérêts du VPN, contrôle du point d'accès

LES ARCHITECTURES DE CLOISONNEMENT

- ▶ La sécurité des VLAN et hébergements, DMZ et échanges, sécurisation des tunnels, VPN Peer to Peer et télé accès, de la sécurité périphérique à la sécurité en profondeur

LA SÉCURITÉ DES END POINT

- ▶ Le durcissement : postes de travail, ordi phones, serveurs
- ▶ L'adjonction d'outils : postes de travail, ordi phones, serveurs
- ▶ La sécurité des applications : les standards et les bonnes pratiques



Formation État de l'art de la sécurité des Systèmes d'Information

Définition de la politique de sécurité et maîtrise des risques

Objectifs de cette formation

- ▶ Appréhender les concepts fondamentaux de l'analyse de risques SSI
- ▶ Savoir identifier les enjeux
- ▶ Disposer d'une démarche complète pour mener à bien un projet d'analyse de risques
- ▶ Découvrir les méthodes d'analyse et les solutions logicielles disponibles pour maîtriser les risques du SI

Programme

LES CONCEPTS GÉNÉRAUX DE LA GESTION DES RISQUES

- ▶ Définition du risque et des typologies de menaces
- ▶ Modèle général de gestion des risques

LES CONCEPTS GÉNÉRAUX DE LA GESTION DES RISQUES

- ▶ La gouvernance à prévoir, les acteurs, leurs rôles et responsabilités
- ▶ La voie hiérarchique et les voies fonctionnelles
- ▶ Identification des risques juridiques : métier, civil, pénal, réglementaire, contractuel

- ▶ Identification des risques accidentels
- ▶ Identification des risques d'erreurs
- ▶ Identification des risques liés à la malveillance (cybercriminelle, concurrentielle, ludique, idéologique et stratégique) : les caractéristiques de compétence, temps, moyen, connaissance au préalable sur la cible, ...

PRÉSENTATION DE LA NORME ISO 31000

- ▶ Objectifs de la norme

PRÉSENTATION DE LA NORME ISO 31000

- ▶ Objectifs de la norme
- ▶ Présentation du contenu de la norme
- ▶ Démarche générale de l'analyse des risques
- ▶ Démarche d'appréciation et d'analyse des risques
- ▶ Classification
- ▶ Les pièges à éviter
- ▶ Présentation des référentiels d'analyse des menaces, des enjeux et des contraintes : la granularité et les domaines d'analyse
- ▶ Présentation des référentiels de vulnérabilité proposés par la norme
- ▶ Présentation des métriques d'appréciation des risques : les approches possibles
- ▶ La stratégie de traitement des risques, les objectifs et l'acceptation des risques selon la norme
- ▶ Les processus de communication et de surveillance des risques
- ▶ Les validations EIVP
- ▶ Les homologations RGS, PSSix

PRÉSENTATION DE LA NORME ISO 31000

- ▶ Objectifs de la norme
- ▶ Présentation du contenu de la norme
- ▶ Démarche générale de l'analyse des risques
- ▶ Démarche d'appréciation et d'analyse des risques
- ▶ Les validations AIPD

LES HOMOLOGATIONS RGS, PSSIX

- ▶ Objectifs
- ▶ Présentation du RGS
- ▶ Démarche d'homologation...

ÉTUDES DE CAS

LA PRISE EN COMPTE NATIVE DES RISQUES SSI DANS LES PROJETS

- ▶ L'approche en V
- ▶ L'approche Agile
- ▶ EBIOS
- ▶ EBIOS RM
- ▶ MEHARI
- ▶ Adaptée
- ▶ La déclinaison Privacy by design du RGPD

ÉTUDES DE CAS

LA DÉFINITION ET LA MISE EN OEUVRE DU PLAN DE PRÉVENTION DES RISQUES (PPR)

- ▶ Notions principales et objectifs du PPR
- ▶ Le processus d'élaboration du PPR
- ▶ La définition des objectifs et des priorités de mise en oeuvre
- ▶ Introduction à la norme ISO 27002
- ▶ Le cas du Cloud ISO 27018
- ▶ Les relations avec les PCA et la norme 22301
- ▶ Les relations avec la gestion de crise

LES CONSEILS DE MISE EN OEUVRE D'UNE GESTION STRUCTURÉE DES RISQUES

- ▶ La gouvernance
- ▶ La mise en oeuvre du système de management de gestion des risques
- ▶ Le maintien en condition opérationnelle

LA PRISE EN COMPTE DU FACTEUR HUMAIN DANS LA GESTION DU RISQUE SI

- ▶ Direction générale
- ▶ Encadrement
- ▶ Acteurs DSI
- ▶ Représentant de la MOA
- ▶ Les utilisateurs
- ▶ Les solutions
- ▶ Études de cas

LES PRINCIPES GÉNÉRAUX RELATIFS AUX SYSTÈMES DE MANAGEMENT DE LA SÉCURITÉ

- ▶ Le système de management ISO 31000
- ▶ Présentation générale du modèle PDCA ISO 27001



Formation Auditer et contrôler la sécurité du SI

Assurer le suivi de la sécurité

Objectifs de cette formation

- ▶ Être capable de construire les indicateurs et les tableaux de bord nécessaires à l'audit et au suivi de la sécurité du SI
- ▶ Connaître les enjeux et les obligations en matière de pilotage de la sécurité
- ▶ Disposer d'une méthodologie d'audit de la sécurité
- ▶ Comprendre comment réaliser des tableaux de bord parlants et efficaces
- ▶ Pouvoir maîtriser les techniques de contrôle de la sécurité des SI

Programme

INTRODUCTION : RAPPEL SUR LES ENJEUX ET LES OBLIGATIONS EN MATIÈRE DE PILOTAGE DE LA SSI

- ▶ Définitions
- ▶ Rappel sur les principes d'un système de management de la SSI (ISO 27001)
- ▶ Les exigences réglementaires et légales en matière de pilotage de la SSI

LES CONCEPTS GÉNÉRAUX DE LA GESTION DES RISQUES

- ▶ Rôles et responsabilités des acteurs impliqués dans la SSI (Direction générale, Directions métiers, DSI, RSSI, DPO, RPCA, Auditeur, contrôle interne, ...)
- ▶ Les instances de décisions
- ▶ La gouvernance à prévoir dans le cadre du pilotage et du suivi de la SSI

AUDIT DE LA SÉCURITÉ DES SI

- ▶ Les catégories d'audit (audit de configuration, tests intrusifs, audit de code, ...)
- ▶ Les recommandations de l'ANSSI (Guide PASSI)
- ▶ La démarche à adopter par l'auditeur (préparation de la mission, réalisation de la mission, restitution de la mission, métriques, ...)
- ▶ L'audit dans le cadre de la sous-traitance
- ▶ La certification des auditeurs
- ▶ La prise en compte des résultats de l'audit par l'organisme (arbitrage, amélioration des dispositifs opérationnels, ...)
- ▶ Les indicateurs de suivi des audits

AUDIT DE LA SÉCURITÉ DES SI

- ▶ Les catégories d'audit (audit de configuration, tests intrusifs, audit de code, ...)
- ▶ Les recommandations de l'ANSSI (Guide PASSI)
- ▶ La démarche à adopter par l'auditeur (préparation de la mission, réalisation de la mission, restitution de la mission, métriques, ...)
- ▶ L'audit dans le cadre de la sous-traitance
- ▶ La certification des auditeurs
- ▶ La prise en compte des résultats de l'audit par l'organisme (arbitrage, amélioration des dispositifs opérationnels, ...)
- ▶ Les indicateurs de suivi des audits

TABLEAUX DE BORD DE LA SÉCURITÉ DES SI

- ▶ Les démarches proposées (normes ISO 27004, démarche proposée par l'ANSSI, démarche proposée par le CIGREF, ...)
- ▶ Les catégories d'indicateurs SSI de niveau stratégique et opérationnel
- ▶ La construction et l'alimentation des tableaux de bord SSI
- ▶ Le traitement des écarts (identification des non-conformités, définition des mesures correctives, ...)

CONTRÔLES DE LA SÉCURITÉ DES SI

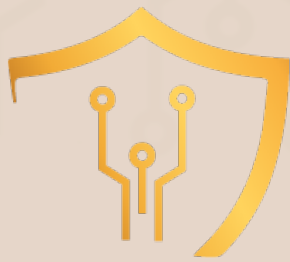
- ▶ Les contrôles permanents de la SSI (détections d'intrusion, gestion des logs, journalisation, ...)
- ▶ Les contrôles périodiques de la SSI (enquêtes, gestion des traces, ...)
- ▶ Les revues de direction (démarche, objectifs, ...)

LA PRISE EN COMPTE DES AUDITS, TABLEAUX ET CONTRÔLES DE LA SSI DANS LES DÉMARCHES PROJETS

- ▶ La démarche GISSIP proposée par l'ANSSI
- ▶ Les nouvelles règles Européennes imposées par le règlement Européen (Privacy By Design)

ÉTUDE DE CAS

- ▶ Mise en oeuvre de tableaux de bord SSI



EXUNOV



+229 65 78 23 78



contact@exunov.com



Pour plus d'informations

www.exunov.com

